DDOS REPORT Q1 2021

The exponential boom in cybercrime will outlast the pandemic. In a post-COVID era, businesses and organizations must adapt to a permanently changed threat environment.

DDoS Attacks that Made Headlines in Q1 2021

Server mit Anfragen geflutet

Cyber-Angriff auf Thüringer Impfportal

07.01.2021

Auf das Thüringer Terminvergabeportal für die Corona-Impfungen hat es laut dem Gesundheitsministerium einen Cyberangriff gegeben.

Erneut massive Serverprobleme beim Distanzunterricht

Der Start ins neue Schuljahr verlief vielerorts holperig. Immerhin scheinen die Kultusministerien langsam zu verstehen, dass zu lange zu viel versäumt wurde.

Lesezeit: 2 Min. In Pocket speichern

SUPERWAHLJAHR IN DEUTSCHLAND

Cyber-Bedrohungen überschatten Bundestagswahlkampf

Hacker-Angriffe und Desinformations-Kampagnen könnten die Bundestagswahl beeinflussen, warnen Experten. Erste Vorfälle zeigen: Die Bedrohung ist real.

Jedes Mal, wenn Delegierte online zur Wahl schritten, nahmen die Angriffe zu. Als die CDU im Januar im Netz eine neue Parteiführung wählte, versuchten Hacker mit einer Serie massiver Cyber-Attacken, den Internet-Parteitag ins Chaos zu stürzen. Wiederholt bombardierten die Angreifer, größtenteils aus dem Ausland, die Webseite der Partei mit Internetverkehr, um ihren Server in die Knie zu zwingen. Mit Erfolg: Irgendwann kollabierte die Seite. Der Live-Stream der Veranstaltung fror ein.

CDU • RND exklusiv • Hacker

Hackerangriff auf CDU-Parteitag womöglich aus Russland

12. Januar 2021 um 16:00 Uhr

RP+ Corona-Pandemie

Hackerangriff auf Schulplattform sorgt für Homeschooling-Chaos am Niederrhein

FURCHT VOR ANGRIFFEN 24.01.2021, 16:30 Uhr

Impfzentren und Impfstoff-Hersteller im Visier von Hackern

Von Rena Lehmann

Foto: dpa

Die Bundesregierung ist alarmiert: Sie warnt vor Hackerangriffen auf Impfstoff-Herstelle und Störaktionen rund um den Start der Impfzentren.

Auch Angriffe auf Stadt Fulda

Hacker attackieren Internet-Portal fürs Homeschooling

Aktualisiert am 14.01.21 um 16:38 Uhr

Industries under Heavy DDoS Fire

Healthcare

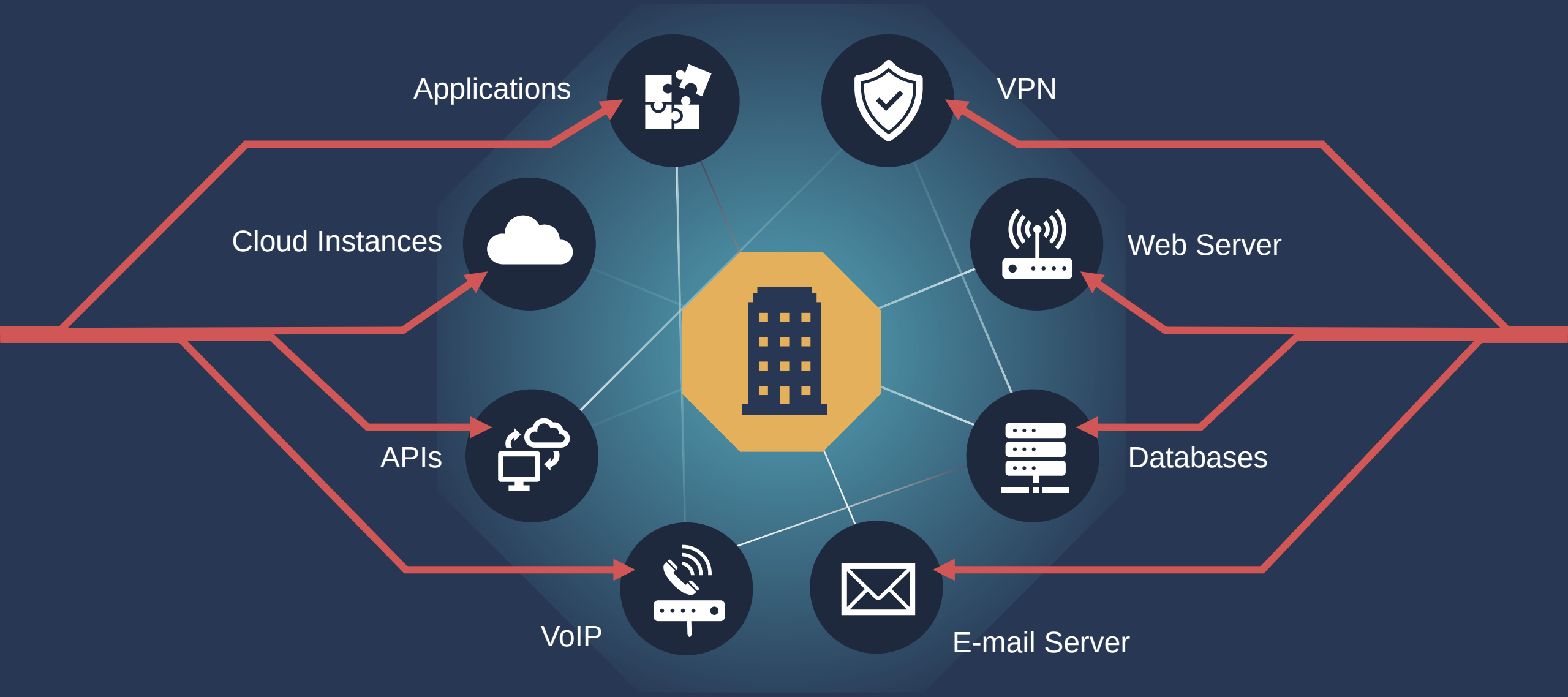
Education

Hosting and Cloud Providers

Logistics

Online Retail

A Growing Range of Vulnerable IT in Companies



3 Attack Trends are Emerging

The number of attacks continues to increase

Attack volume remains high

DDoS attackers stick to their target, even if unsuccessful

DDoS Threat Landscape in Key Figures

+128
%
increase in the number of attacks compared to Q1 2020 (factor approx. 2.3)

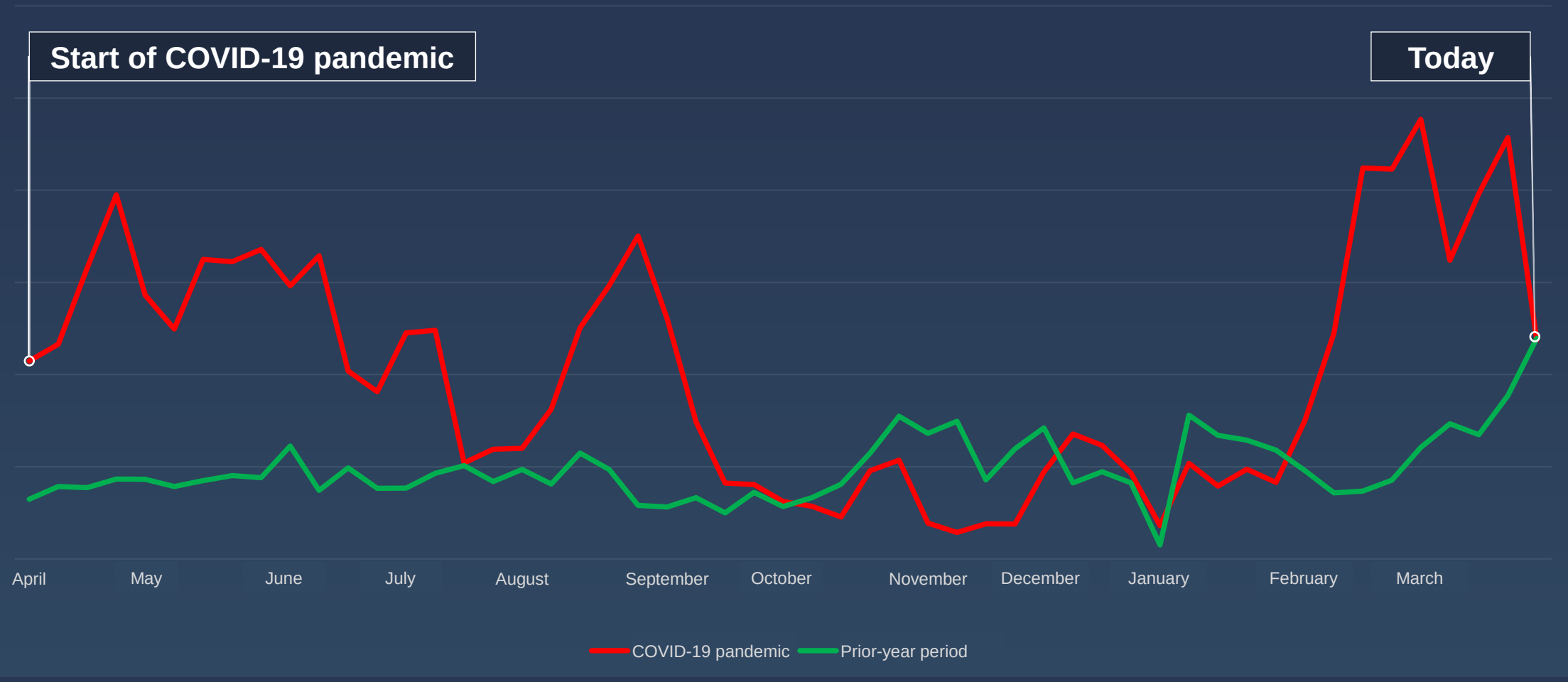
216
Gbps
maximum in attack volume

44
million
packets per second peak in packet rate

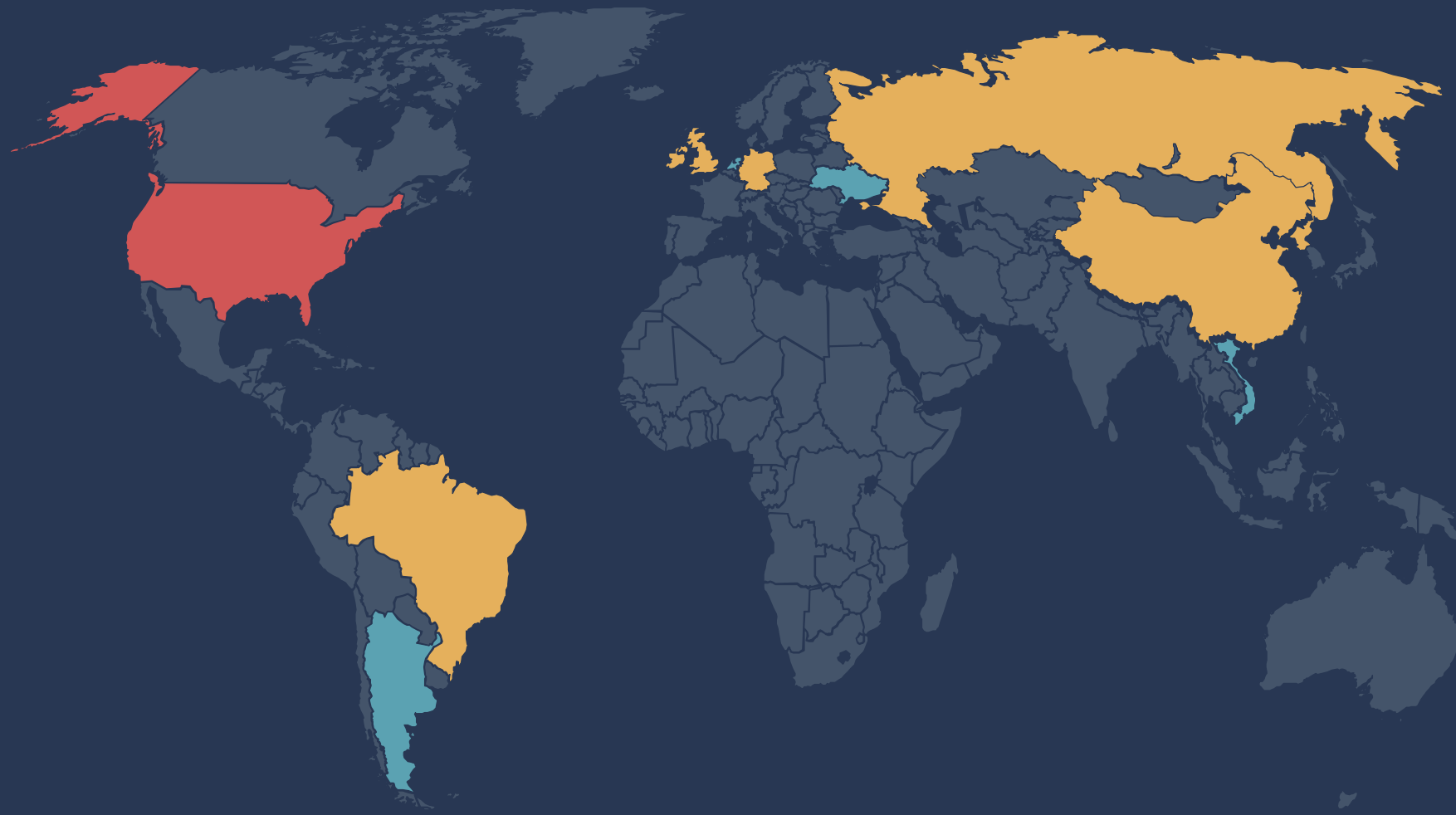
1,489
minutes
the longest duration of an attack (>24 h)

69
%
of attacks were multi-vector attacks

Developments in Attack Numbers before and during COVID-19 Pandemic



Top 10 Source Countries for Reflection Amplification Attacks



USA	31,8%
Germany	9,6%
China	6,5%
Great Britain	5,6%
Brazil	5,5%
Russia	5,3%
Ukraine	3,4%
Netherlands	3,4%
Vietnam	2,5%
Argentina	2,4%

Hosting Providers Targeted by DDoS Attacks

47%

of all registered attacks in Q1 2021 were targeted at data center operators and hosting providers

The most common attacks included:

- Carpet Bombing attacks
- High volume attacks
- DDoS extortion

About the Report

Methodology

The Link11 DDoS report Q1 2021 is based on data from the monitoring of Link11's global network. The staved-off attacks targeted websites and servers protected against DDoS attacks by Link11. The data was collected from January 1 to March 31, 2021. Due to a change in the methodology used to identify and count attacks in 2020, the data is not comparable to statistics cited in previous reports. Besides network analyses and evaluating DDoS attack data, the Link11 DDoS report also utilizes open-source intelligence (OSINT) analyses.

About Link11

Link11 is the leading European IT security provider in the field of cyber-resilience headquartered in Germany, with sites worldwide in Europe, North America, Asia and the Middle East. The cloud-based security services are fully automated, react in real-time and defend against all attacks, including unknown and new patterns, in under 10 seconds. According to unanimous analyst opinion (Gartner, Forrester) Link11 offers the fastest detection and mitigation (TTM) available on the market. The German Federal Office for Information Security (BSI) recognizes Link11 as a qualified DDoS protection provider for critical infrastructures.

To ensure cyber-resilience, web and infrastructure DDoS protection, Bot Management, Zero Touch WAF and Secure CDN Services among others provide holistic and cross-platform hardening of business' networks and critical applications. The 24/7 operated Link11 Security Operation Center, which is located at sites in Germany and Canada according to the follow-the-sun principle, provides the reliable operation of all systems and manages the expansion of the global MPLS network with 41 PoPs and more than 4 Tbps capacity. Guaranteed protection bandwidths of up to 1Tbps provide maximum reliability. International customers can thus concentrate on their business and digital growth. Since the company was founded in 2005, Link11 has received multiple awards for its innovative solutions and business growth.

Photo Credits: Shutterstock ID 504234469 (cover), iStock ID 1226864145 (p 10)

Graphics: Link11 GmbH

CONTACT

Link11 GmbH
Lindleystr. 12
60314 Frankfurt

info@link11.com
+49 69 264929777